NATIONAL SECURITY FELLOWS PROGRAM

A Next Generation National Information Operations Strategy and Architecture

Jack Kiesler

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
SEPTEMBER 2021

National Security Fellowship Program
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/NSF

Design by Andrew Facini
Layout by Benn Craig

Printed in the United States of America

NATIONAL SECURITY FELLOWS PROGRAM

A Next Generation National Information Operations Strategy and Architecture

Jack Kiesler

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JULY 2021

About the Author

Jack Kiesler is a national security professional with expertise in defense and military intelligence. Much of his career has been dedicated to counterintelligence activities associated with cyber, technical, and information operations. In 2021, Jack successfully completed the National Security Fellowship at the John F. Kennedy School of Government, Harvard University. While there, he studied a broad array of pressing domestic and global issues concerning U.S. national security policy, centering his research on information operations, foreign policy and artificial intelligence.

Jack Kiesler currently works for the Defense Intelligence Agency in Washington D.C., where he has held positions at the Office of the Director of National Intelligence, the National Insider Threat Task Force, and U.S. Cyber Command. Prior to working at the Defense Intelligence Agency, Jack served as an officer in the U.S. Air Force. During his 20 year military career, he served as a counterintelligence special agent commanding investigations, collections, and operations across Europe, Asia, and the Middle East.

Acknowledgements

I'd like to specifically thank both Major General William E. Rapp (Ret.), Director of the National Security Fellowship and General Joseph F. Dunford (Ret.), former Chairman of the Joint Chiefs of Staff. Their motivation, insights and expertise were invaluable.

This paper could not have been possible had it not been for the large number of information operations professionals across the community who contributed their thoughts and experiences to help forward the development of this new strategy. These professionals are senior leaders across the Department of Defense and the Intelligence Community, as well as senior executives in the defense industry. Several of our findings compete with historical convention, which has led to a new paradigm on how to combat adversarial information operations. My gratitude for their contributions can not be overstated. Their acknowledgement remains private.

Lastly, I'd like to thank my family for their support and patience. Specifically, I'd like to thank my father, who has since passed, who had guided me into a life of service as well as my mother who has always been my rock. My two grown children (Lauren and Ryan) have always been an inspiration, providing innovative and critical thought to the most complex international issues. Finally, I'd like to thank my wife, Angie, who continues to impress me with her unyielding love and support. She is my own personal hero, my muse.

Table of Contents

Real-time cyber attacks, including information on the attack's origin, type and target, as well as, the attacker's IP address, geographic location and ports being utilized, are displayed on the Norse attack map on the 275th Cyberspace Squadron's operations floor, known as the Hunter's Den, at Warfield Air National Guard Base, Middle River, Md., June 3, 2017.

J.M. Eddins Jr./Air Force

The Reckoning

It is 0400 hours EST on March 27, 2019, and the power goes out. It's utterly dark across the city. I call my wife to see if she's heading home from her midnight shift as a registered nurse at a local hospital. However, the dial tone is inaudible. The phone lines are down across parts of northeast United States. In this scenario, I am a liaison officer from the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security assigned to the United States Cyber Command. I decide to head into the office quickly. As I pull into Fort Meade, I see the traffic is heavier than usual. The back-up generators power the buildings, and the place is humming with activity, there's great tension.

I reach my office, which is assigned the responsibility of conducting cyber operations analysis. There's too much data to quickly attribute the source and the associated tactics. However, one thing is clear. This attack has the signature of the Chinese. It appears they have exploited the loosely monitored acquisition lifecycle to manipulate the electric and power critical infrastructure sector's supply chain (See Figure One). The Chinese have hacked these proxy servers, in order to quietly hijack, and establish a virtual foothold in the United States. The intent is to lead the United States in believing the attack may be coming from a perceived United States citizen, providing China plausible deniability, as well as exploiting United States intelligence oversight laws.

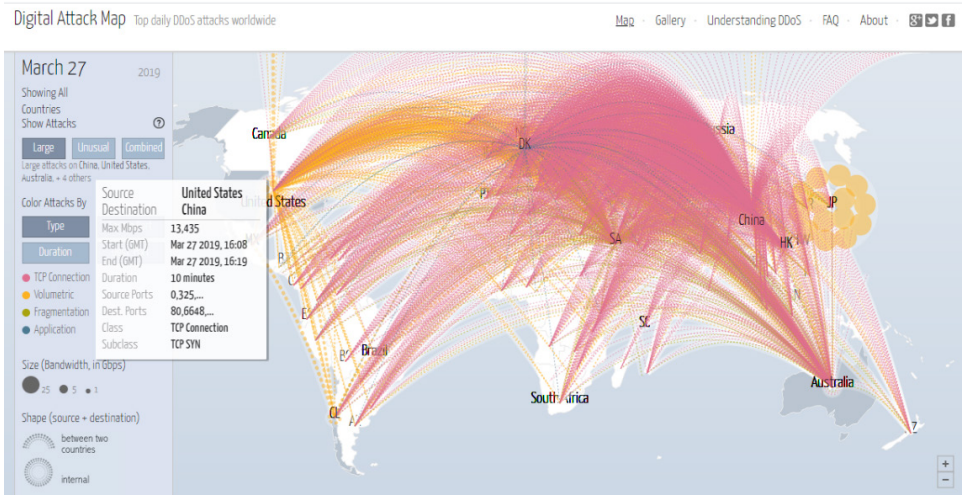

Figure One: Digital Attack Map (Scenario) *Source: Digital Attack Map*

After several hours, a common operating picture comes into view revealing a distributed denial-of-service attack had occurred at unprecedented levels targeting the northeast United States power grid, along with specifically targeting associated network connectivities with both US Cyber Command and the Department of Homeland Security's own infrastructure. This attack was clearly designed to hinder investigative and response actions.

Synchronized with the timing of these network attacks are mundane stories dominating mainstream and social media of Xi Jinping visiting France. The headline '*Historic Tour of Europe*' was viewed by the masses. These benign stories of China's interest in creating its equivalent of Hollywood were essentially an effort to project the impression that everything's calm in China: "These network attacks aren't us." This is all part of Chinese information operations.

In Asia, China transitions the storyline to flooding social media with disinformation that it is rescuing Taiwan from emergent social unrest. Soon thereafter, breaking news: China's Xian H-6 bombers and accompanying Chengdu J-20 fighter jets have breached the Taiwan Strait median line, providing top cover for its special forces to gain a foothold in Taiwan. President Xi's design to lull the larger global public, while concurrently conducting network attacks to disrupt and dissuade, has successfully achieved the multi-dimensional information operations effect for China to intervene in Taiwan.

China's information operations campaign began years earlier. Stories within the press reflecting initial acquiescence in maintaining the status quo with Taiwan, covert compromise of the Taiwanese information technology supply chain, conducting military exercises involving peacekeeping to the West to quiet expectations, and increased private sector collaboration with Taiwan, were all elements of China's multi-dimensional Information Operations[1] campaign. Like chess, each piece of national power was manipulated through cyber operations, disinformation

[1] Since 2006, particularly within US DOD, the distinction between Information Operations (IO) and Information Warfare (IW) remains less clear. For the purpose of this paper, the author will use IO exclusively to address the full range of capabilities, exercised during either gray zone activities or during war. JP 3-13 characterizes IO as "the integrated employment of information-related capabilities to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."

campaigns, active measures, and influence operations, all to achieve strategic surprise to meet national objectives. Some levers of national power were employed to provide strategic advantage, others to lull.

The Thesis

There are four recognized instruments of national power; diplomatic, *informational*, military, and economic, creating the acronym DIME. The phrase *instruments of national power* refer to the tools a country uses to influence other countries or international organizations or even non-state actors. *Information* is a core, primary instrument of national power, yet ironically, the "I" in DIME continues to remain silent, under-resourced, and under-used as an element of United States national power.

Most paradoxically, the United States dramatically excels at most elements of informational power: public diplomacy, public affairs, soft power (cultural influence), communication resources (media and social media), international forums, spokespersons, etc.[2] However, the United States cannot seem to harness this to achieve strategic national objectives. Rarely are the elements of informational power synchronized to achieve national objectives to the same degree, dedication, and sophistication found within China and Russia. These countries don't hesitate to target our critical infrastructure and supply chains and virally spread lies to damage our democracy, security, and even public health. We need an equally multi-dimensional response.[3]

This research paper conducts a deep dive into sources and includes interviews of senior information operations professionals to broadly identify strategic gaps in capability that continue to plague America's information operations. Through interviews with key members affiliated with the national information operations community, I outline and propose a new strategy and architecture. If supported and built, it can provide the capability to unleash America's informational power and help achieve national strategic objectives.

Stipulating in advance of the findings to follow within this research, the appointment of a National Information Operations Director would assuredly be met with criticism. However, this critical first step would

2 "Instruments of National Power," *The Lightning Press SMARTbooks* (blog), September 20, 2014, https://www.thelightningpress.com/the-instruments-of-national-power/.

3 Peter Singer (author of Ghost Fleet) in discussion with the author, February 25, 2021.

dramatically move the nation's public discourse and lead to a new, homogenized system of capabilities that are available to meet national objectives. The proposal must be led by a non-partisan 'dream team,' as the public's wariness of the government's intent to deploy Information Operations, in spite of its noble purpose, would be met with skepticism. However, with strong leadership, along with direct public support and teaming, criticisms can be assuaged.

Once the strategy is viewed as protecting our democratic ideals, the public will slowly recognize its value and become part of the solution. Further, checks and balances to prevent political interests from influencing decision-making, marketing the intent, along with strong legal reviews, are also critical elements to combat public concern.

Ringing the Bell

Many within the United States security and the Intelligence Community have been ringing the bell for quite some time. According to the 2018 Department of Defense Cyber Strategy, China is eroding the United States military overmatch by persistently exfiltrating sensitive information from the U.S. public and private sector institutions, and conducting disinformation, active measures, and influence operations.[4] The Chinese construct on *Informationized Warfare*[5] extends to a whole-of-nation approach to include leveraging professional relationships, exploiting universities, think tanks, and media. The United States cannot afford to continue thinking that its economic and military might always give its adversaries pause. We are now at our reckoning.

Admiral Mike Rogers, then Commander, US Cyber Command, agreed with a Defense Science Board finding during a 2018 Senate Armed Services Committee Hearing. He proclaimed that "for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to exceed the United States' ability to defend key critical infrastructure."

Just as concerning, Russia continues to barrage the American public with sophisticated measures to influence our population and challenge our democratic processes, seeking to sow discord. The Kremlin's influence operations employ state and non-state resources to achieve their ends to execute a multi-dimensional approach that involves security services, television stations, pseudo-news agencies, social media and internet trolls, public and private companies, organized crime, think tanks and special foundations, and social and religious groups. Their weapon of choice is the influence operation. According to reporting, "our goal wasn't to turn the Americans toward Russia. Our task was to set Americans against their Government: to provoke unrest."[6]

---

4 "2018 Cyber Strategy Summary," accessed October 20, 2020, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/Cyber_Strategy_Summary_Final.pdf.

5 Timothy L. Thomas, *Dragon Bytes: Chinese Information War Theory and Practice* (Fort Leavenworth, Kan.: Foreign Military Studies Office, 2004).

6 Bob Corker et al., "Committee on Foreign Relations," n.d., 206.

Other actors, such as North Korea and Iran, are certainly not absent. Both have similarly employed information operations activities to harm United States citizens and threaten its' interests.[7] Both North Korea and Iran are often proxies and collaborators of China and Russia, both used to distract, "echo or seed" disinformation, initiate computer network operations, and other forms of active measures. Hereafter, these four countries combined will be collectively referred to as the "*Four Information Operations Adversaries*."

7 "2018 Cyber Strategy Summary."

Information Operations Environment

The information environment comprises and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and affect knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization (Figure Two). The information environment directly affects and transcends all operating environments and is where information operations reside.[8] This, therefore, becomes the information operations environment.

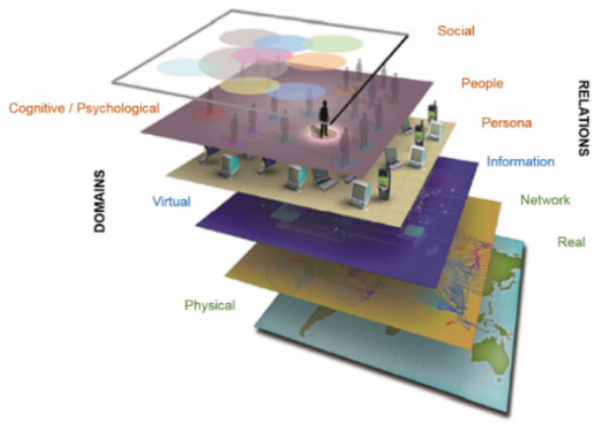

Figure Two: Information Environment

The necessity of fusing cyber operations with that of protecting and projecting information (via deception, psychological operations, operations security, etc.) has mostly been recognized as a necessity within information operations evolution. National information operations' leadership has recognized this dynamic, professing that you can't remove the "means" (cyber) from the "ends" (cognitive/influence) - they are inextricably tied as a single, synergistic "platform." Further, information operations consist of both offensive and defensive activities; each inform the other. *Information operations are the protection and assurance of one's information while enabling and executing an*

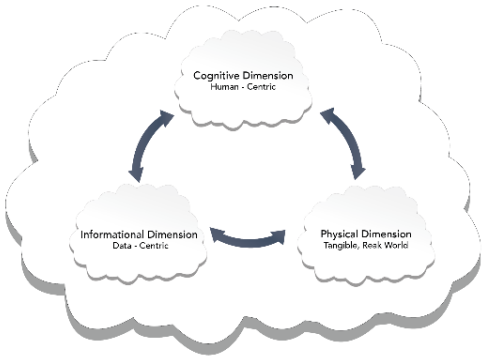

Figure Three: Information Environment *Source: JCOIE*

8 "Joint Concepts - Operating in the Information Environment.Pdf," accessed December 31, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.

information advantage.[9] This more-unified capability must begin to dominate discussion within the United States in order to protect and combat nation-state foreign influence and exploitation, which includes the cognitive, human element of the information domain. This is where much nation-state, adversarial activity occurs, particularly in the Gray Zone.[10]

Having the full range of information operations capabilities (Figure Four) considered during defensive and offensive activities, to support campaign plans, would securely return the "I" in DIME. These are the core building blocks normally associated with information operations.

Activities that *project* and *protect* information at the national level include:

Figure Four: Information Operations Construct *Source: Joint Publication 3-13, brown boxes added by author.*

traditional and social media, diplomacy and forums. The author added these brown boxes (Figure 4 above), to a pre-existing Joint Publication 3-13 image of how the Department of Defense captures information operations, to highlight the broader national level activities.

9 "Joint Publication 3-13.Pdf," accessed December 7, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

10 "Joint_concepts_JCOIE.Pdf."

Snapshot of Evolving Threat Landscape

Over the course of the last 20 years, the United States has fallen victim time and again, from the ability of the *Four Information Operations Adversaries'* to evolve and mature their information operations capabilities. They clearly understand the full scope of the information operations environment:

In 2003, *Titan Rain*, originating in China, gained access to many United States defense contractor computer networks of the defense industrial base to pilfer intellectual property. Never has so much of a nation's military edge been blunted than in the last two decades.

In 2016, Russian expanded its offensive strategy to promote discord and call into question the legitimacy of democratic institutions in the United States/Western Europe. These measures have included providing financial support to extremist groups, disinformation campaigns, and trolling.[11]

In 2020, influence operations remain persistent. The opposed statements that 'the United States military brought COVID-19 to Wuhan, China,' is an example of disinformation packages spread by China, Iran, and Russia mostly designed to confuse and further divide the United States population and undermine trust in United States democratic processes.

[11] Charles E. Ziegler, "International Dimensions of Electoral Processes - Russia, the USA, and the 2016 Elections," *International Politics* 55, no. 5 (September 1, 2018): 557–74, https://doi.org/10.1057/s41311-017-0113-1.

Adversarial Advantages *Four Information Operations Adversaries'* Possess

Each of the *Four Information Operations Adversaries'* possess authoritarian governments which provide government institutions the ability to direct a whole-of-nation approach.[12] Each can exercise influence within their public, press, or a skeptical and potentially powerful electorate, to achieve information operations objectives without delay. The Democracy Index, produced by the Economist Intelligence Unit, gives China and Russia a 2.26 and 3.11 respectively, out of 10. The Democracy Index classifies their Governments as clearly authoritarian.[13] Both countries have seeded and tasked patriotic movements within their countries to generate organic information operations capabilities. This helps them proclaim plausible deniability when conducting information operations. They can pull the levers of national power associated with DIME[14] instantly, often leveraged to confuse public opinion, paralyze political decision-making, subvert legal frameworks, and avoid crossing the military response threshold by their adversaries.[15]

The Gray Zone is the environment that the *Four Information Operations Adversaries* prefer operating, as each would be at a distinct disadvantage should traditional conflict against the United States emerge. The 2018 Joint Concept for Integrated Campaigning replaces what is now considered an obsolete peace/war 'binary' with a new model of conflict which includes 'below' warfare – the Gray Zone.[16] The Gray Zone involves unwritten rules-of-engagement and takes advantage of the United States' inability to classify an activity as warfare.

---

12 Catherine A Theohary, "Information Warfare: Issues for Congress," *Information Warfare*, n.d., 19.

13 "Democracy in China," in *Wikipedia*, December 13, 2020, https://en.wikipedia.org/w/index.php?title=Democracy_in_China&oldid=993952049.

14 D.I.M.E. (the four national instruments of power; diplomacy, informational, military, and economic)

15 "Joint Concept Integrated Campaign.Pdf," accessed January 4, 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.

16 "Joint Concept Integrated Campaign.Pdf."

Further, the *Four Information Operations Adversaries* also have the ability to exploit the United States' legal system. As a nation of laws, the United States often defaults to *responsive caution* to prevent inadvertent violation of privacy, intelligence oversight, etc. The exploitation of United States laws has yielded dramatic success for the adversary. Often, an adversary will quietly target a benign system within the United States, serving as a proxy, to then launch an attack on their intended target. This is to exploit the United States 'domestic' intelligence collection conundrum, in spite of perceived foreign sources.

Five Strategic Gaps... Findings of Research

To combat these adversarial advantages, the United States must recognize it must fill five persistent gaps that handicap its ability to execute successfully information operations. These five strategic challenges continue to generate lingered, uni-dimensional, and uncoordinated responses that leave tremendous capabilities on the table. Below are five gaps that have consistently emerged during the interviews of senior information operations professionals. Each gap highlights key data points to help shape the development of *A National Information Operations Strategy and Architecture* which follows this section.

1. No Recognized Leadership for National Information Operations Architecture

There is no recognized leadership to task, direct, resource, or guide policy in the highly complex, disparate field of information operations. As a consequence, pockets of excellence have emerged in the past to provide the country with instances of success. However, these occasions were accomplished in spite of, not because of, a national vision or leadership to harness national strengths to meet its objectives. Below are data points to highlight the lack of a national information operations leadership and strategy as a gap:

- During the Cold War, the United States Information Agency was responsible for supporting United States national interests abroad through information dissemination. The State Department's Bureau of Public Diplomacy and Public Affairs assumed United States Information Agency's mission before it too was disbanded in 1999.
- The Department of State-led Global Engagement Center has a vital role in support of information operations. Although this role is a fraction of the entirety of information operations, as well as the Center is grossly under-resourced. The Global Engagement Center

is responsible for many former United States Information Agency activities. The Global Engagement Center received these new responsibilities partly due to Title 10, USC 2241, which prohibits the Department of Defense from domestic publicity or propaganda. At present, the Global Engagement Center, charged with "leading the United States Government's efforts to counter propaganda and disinformation from international terrorist organizations and foreign countries" has limited resources and capacity. According to Thomas Hill, a former House senior staffer, "If people were serious about combating Russian propaganda, you have to be honest -- $80 million and 50 people in the basement of the State Department are not going to cut it. That is not enough." A January 2018 United States Senate report specified, "In early 2017, Congress provided the Global Engagement Center the resources and mandate to address the Kremlin disinformation campaigns. Operations, though, have been hindered by the Department's hiring freeze and unnecessarily long delays by its senior leadership in transferring authorized funds to the office."

- The Central Intelligence Agency has a mission responsibility that would be at odds for being the 'face' of a national information operations capability. Although according to a Congressional Research Service report dated March 5, 2018, entitled "Information Warfare: Issues for Congress," the Central Intelligence Agency has a history of conducting information operations or psychological operations. Monitoring Soviet disinformation was once solely the CIA's purview until the Active Measures Working Group was established in 1981 and tasked with coordinating multiple, disparate activities within the United States government. Their role would assuredly be core, but not leading the national architecture.
- Also of note, the fiscal year 2020 budget requests $1.608 billion in appropriations for all of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency activities. The Cybersecurity and Infrastructure Security Agency mission in cybersecurity and infrastructure protection is focused on enhancing greater collaboration on cybersecurity across the 16 critical infrastructure sectors and sharing cyber threat information

between the private sector and Federal, State, and local partners. They, too, would have a key role, however, the Cybersecurity and Infrastructure Security Agency would center their activities in a defensive capacity, along with the development of fusion centers for analysis.

- Most surprising, at present, there isn't a recognized United States Department of Defense lead to resource, develop policy, guide and coordinate information operations. CJCS Instruction 3210.01, Joint Information Operations Policy, proclaims authority to conduct joint information operations being vested in the combatant commander, who in turn can delegate operational control to a subordinate Joint Force Commander, as appropriate. Unfortunately, information operations do not retain geographic, or even functional boundaries. Nor can information operations await delegation from a combatant commander.

- The Joint Information Operations Warfare Center supports combatant command electronic warfare, a key element of information operations. Electronic Warfare, such as jamming command and control systems, satellites used for global positioning systems, and radio communications, remains distributed across the Services and yet is a key feature in Department of Defense information operations.

- The Secretary of Defense directed US Special Operations Command to establish a centralized Department of Defense Military Information Support Operations (previously called Psychological Operations) global messaging and counter-messaging capability, with $1.8 million allocated in FY 2019 for the initiative.[17] Again, well intended, but another stovepipe.

- Generating additional pockets of capability, the military services have also begun to adapt their organization frameworks to prioritize information operations, albeit inconsistently. For example, the Marine Corps has a new deputy commandant for information. The Air Force previously had separate numbered

[17] Ben Hatch, "The Future of Strategic Information and Cyber-Enabled Information Operations," *Journal of Strategic Security* 12, no. 4 (January 2019): 69–89, https://doi.org/10.5038/1944-0472.12.4.1735.

Air Forces for cyber and intelligence functions but consolidated them in 2019 under the 16th Air Force/Air Forces Cyber. While remaining cyber-centric, the 16th Air Force incorporates other information operations capabilities, including electronic warfare, information operations, and intelligence, surveillance, and reconnaissance.[18] The Navy stood up the Naval Information Warfare Development Center to grow a skilled cadre of information operations professionals for the future battlefronts. The Army established a pilot program to identify where service information operations capabilities should reside, budgeting $14.7 million for training in FY 2019. By late 2021, the Army Cyber Command now focuses on information operations more broadly. Army Cyber Command aims to integrate cyber, information operations, and electronic warfare by 2028.[19] Service-centric capabilities does not create the jointness and unity of effort, particularly in the ubiquitous, transitory information operations environment.

- Finally, in October 2018, US Cyber Command Cyber Strategy Symposium highlighted ongoing information operations challenges, central being the current subdividing information operations and cyberspace capabilities. The Symposium instead proposed solutions focused on what US Cyber Command could do to augment the nation's ability to conduct strategic influence operations rather than moving to oversee information operations.

2. Whole-of-Nation Strategy Remains Hyperbole - Both The Private Sector and Citizenry Have an Increased Role

National efforts to defend from nation-state information operations adversaries, most always reflect a need for a whole-of-nation response. Most achieve strong collaboration when developing response actions. However, several communities warrant additional attention, particularly

[18] "Disruptive by Design: Transcending Cyber," SIGNAL Magazine, January 25, 2021, https://www.afcea.org/content/disruptive-design-transcending-cyber.

[19] Hatch, "The Future of Strategic Information and Cyber-Enabled Information Operations," January 2019.

in the day-to-day execution of defensive information operations. The Department of Defense leverages the Campaign Plan approach, which is effective in helping drive integration. However, at the national level, the private sector and even the public, need to be called out specifically, as there are opportunities. The below are data points that highlight this:

Private Sector

- The 2013 National Infrastructure Protection Plan mandates that sector-specific agencies are "responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms." In addressing the broad, national intelligence challenges in cybersecurity, it is essential to do so in the context of private-sector innovation.[20] The private sector has obligations to its billions of users worldwide, and the Government can directly benefit from private-sector innovation, assuming the right governance structures are in place.[21]

- The Cybersecurity Information Sharing Act of 2015 provides liability protections to private entities that share cyber threat indicators and defensive measures with other private entities and the Government. It protects the confidentiality of the information shared with the United States Government. And yet, relatively few companies outside select sectors are proactively sharing cybersecurity threat information with federal entities.[22] The Cyber Intelligence Sharing and Protection Act; President Obama's 2013 Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity', and the National Institute of Standards and Technology Cybersecurity Framework launched in February 2014, all contribute to increased public and private collaboration.[23]

---

20 "2013 National Infrastructure Protection Plan.Pdf," accessed January 6, 2021, https://permanent.fdlp.gov/gpo147129/national-infrastructure-protection-plan-2013-508.pdf.

21 VA Greiman, "Public/Private Partnerships in Cyberspace: Building a Sustainable Collaboration," *Journal of Information Warfare* 14, no. 3 (2015): 30–42.

22 "FDD | U.S. Government and Private Industry Must Prepare for Cyber-Enabled Economic Warfare Escalations," FDD, February 5, 2019, https://www.fdd.org/analysis/2019/02/05/government-and-private-industry-must-prepare-for-cyber-enabled-economic-warfare-escalations/.

23 Greiman, "Public/Private Partnerships in Cyberspace."

- Highlighting the importance of a whole-of-nation construct, on January 2, 2021, the media released details of an adversarial computer network operations attack targeting a Texas-based company called *SolarWinds*. The attack, affecting 250 federal agencies and businesses, is believed to have originated from Russia. According to a New York Times article, the hackers managed their intrusion from servers inside the United States, exploiting legal prohibitions on the National Security Agency from engaging in domestic surveillance and eluding cyber defenses deployed by the Department of Homeland Security. Most interestingly, the breach was not detected by the Department of Homeland Security, National Security Agency, or US Cyber Command…but by a private cybersecurity company, FireEye, accenting the importance of the private sector role.

Public

- Finally, all citizens must recognize that they have a role in identifying disinformation and reporting suspect network behavior. Much like post-9/11, there was a 'see something – say something' initiative led by the Department of Homeland Security. There's an opportunity here too.

3. No Legal Framework to Advance Information Operations in the Gray Zone

The United States must develop a legal framework more closely reflecting rules of engagement consistent with the environment we've found ourselves in…the Gray Zone. Having a war, or Gray Zone activities be executed at the speed of legal decisions assuredly leave democratic societies at a clear disadvantage. Below captures several data points highlighting this challenge:

- Most authoritarian countries don't dwell over inadvertent and indiscriminate violation of national sovereignty and simply rely on obfuscation and plausible deniability when releasing their information operations' weapons. Indeed, the United States takes pride in maintaining the rule of law. The rules of engagement, though, must ensure response actions can both keep pace with the threat and be unambiguous.
- The NATO Cooperative Defense Centre of Excellence's International Group of Experts prepared the Tallinn Manuals 2.0 (2016), reflecting the consensus view of the International Group of Experts' customary international law applicable to cyber operations. According to Rule 32 of the Tallinn Manual, peacetime cyber espionage does not per se violate international law, although the method by which it is carried out might do so. Jus ad Bellum (right to war) applies to network attacks as well. What constitutes reciprocity at the level of war will have to be weighed. These interpretations are a reflection of the routine gnashing of teeth by attorneys in endorsing aggressive response actions.
- Title 10 USC 2241 authorities prohibits the Department of Defense from domestic "publicity or propaganda." Therefore, the role of the Department of Defense during any form of influence operation will need to be carefully vetted. Cyber weapons and capabilities must be studied to ensure no inherently indiscriminate act occurs (i.e., consistent with the principles of distinction and proportionality).

4. Counterintelligence Decision-Making / Responses Aren't 'Operationalized'

Similar in scope to the above, those possessing counterintelligence authorities need to conduct investigatory and attribution activities at the speed of war fighting operations. The counterintelligence community is often the front line in distinguishing response actions. Therefore, it must be prepared to better operationalize its actions consistent with the environment in which it finds itself - the Gray Zone. Consider:

- Most often, the source of an information operations attack is unknown at the onset. There are precious few moments to react to assure "shields are up" or provide information operations responses. There are laws and procedures to ensure network attacks aren't investigated by the intelligence community if believed to originate from a U.S. person. This helps prevent Intelligence Oversight violations.[24] An adversary knows this and often exploits this by conducting attacks giving the appearance its origination is from within the United States (*Solar Winds et al*). Although the Federal Bureau of Investigation and the Department of Homeland Security have some authority over Internet traffic within the United States, determining attribution can often necessitate a warrant - at the expense of immediate action.

5. Data is Diffused, in Stovepipes, Preventing Big Data Analysis

Today, the United States lags in creating a secured, classified digital framework to support information-sharing relevant to information operations.

- A digital framework that consolidates, analyzes, and even contributes to the decision-making of vast stores of data can achieve remarkable effects with today's artificial intelligence capabilities, such as refuting disinformation, network attack solutions, and so much more. However, at the root of the problem is public trust in the Government to secure and abide by privacy laws, particularly when harnessing enormous amounts of data, some of which may be US Person data.

[24] Executive Order 12333 establishes this balance by prescribing general principles governing intelligence collection, retention and dissemination, and by specifying that intelligence activities concerning U.S. persons may only be conducted in accordance with procedures established by the element or department head and approved by the Attorney General, after consultation with the Director of National Intelligence.

Next Generation National Information Operations Strategy & Architecture

Projecting 'information power' necessitates innovative solutions, guided by a fully resourced and coordinated *Next Generation National Information Operations Strategy and Architecture*. The United States Cyberspace Solarium Commission, in March 2020, co-authored by Senators Angus King and Mike Gallagher, identifies a reflection of the modernity of the cyber security landscape as well as offers recommendations. The Cyberspace Solarium Commission additionally extended discussion to several components of information operations. The 2021 National Defense Authorization Act took many of the findings and incorporated them to help fill gaps within cybersecurity, including a new National Cyber Director at the White House. However, these efforts continue to fall well short of addressing the more complex challenges of a national information operations strategy and architecture. The following strategy is proposed.

1. Designate an Information Operations National Director With Purview Over Cyber

The United States needs an Information Operations National Director, who can rally all elements of information operations community, and who has routine access to the Executive Office of the President. The President's intelligence powers are rather broad. By Executive Order, the President has the authority to conduct global broadcasting in any region at the President's discretion to promote United States policies, achieve United States objectives, and promote democracy.

To date, there is no single individual in the United States government below the President responsible for managing United States information dissemination and providing strategic guidance for how to confront our adversaries in the information environment. A new office must coordinate,

resource, and direct the continued surge in propaganda, misinformation, national-level network attack, deception or disinformation across the information environment.

Figure Five: Nation Information Operations Leadership

Congress should establis Operations Director, supported by an Office of Strategic Narratives, within the President's Executive Office and assign the Department of Homeland Security' Cybersecurity and Infrastructure Security Agency as *"Information Operations-Defense"* and Department of Defense's US Cyber Command as *"Information Operations-Offense."* Congress should establish a House Permanent Select Committee on Information Operations to provide oversight across the Government, ensuring a non-partisan approach, and associated standards are met.

Research published within *Defense One* suggests an Office of Strategic Narratives, resident under the existing Deputy National Security Advisor for Strategic Communications. Leveraging this proposal, along with assigning this office within the Deputy National Security Advisor, their voice will have a direct line to the President and equal footing with the departments that run the various United States messaging programs. [25]

Although the National Defense Authorization Act for Fiscal Year 2021 created the Office of the National Cyber Director within the Executive Office of the President, this position does not include the full breadth of capabilities necessary to support information operations and the associated potentiality for war fighting responsibilities. On 12 April 2021, President Biden announced John "Chris" Inglis as United States's first National

25 "How to Stop Losing the Information War," Defense One, accessed January 8, 2021, https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/.

Cyber Director. According to a recent *Lawfare* article, the National Cyber Director is tasked with predominately defensive responsibilities.[26]

A Director for Information Operations-Defense must also be identified without delay as well, subordinate to the National Information Operations Director. This position is to coalesce both the means and ends (cyber and its cognitive destination) across information operations environment in defense.

The Department of Homeland Security/Cybersecurity and Infrastructure Security Agency should assume this role. However, Cybersecurity and Infrastructure Security Agency should assume an "elevated status" to ensure direct coordination/subordination to the National Information Operations Director. Their role would include cyber deterrence, active cyber defense, offensive cyber actions in support of national cyber defense, incident response, detection of disinformation, foreign information operations targeting, and defensive campaign planning in response to threats. Congress should strengthen Cybersecurity and Infrastructure Security Agency in its mission, authorities, and resources.[27]

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency has developed information-sharing efforts in the critical infrastructure sectors like electricity and financial services that have longstanding mechanisms and channels, including Information Sharing and Analysis Centers. Cybersecurity and Infrastructure Security Agency, in their role as Information Operations-Defense, should fund research on how people and groups are influenced online and should have a partnered relationship with the Department of States' Global Engagement Center.

United States Senators Rob Portman (R-OH) and Chris Murphy (D-CT), via the FY 2017 National Defense Authorization Act Conference Report, authorized the State Department to request $60 million annually for two years from the Department of Defense. Their authorization was designed to support Global Engagement Center funding to counter the

---

26 "Making the National Cyber Director Operational With a National Cyber Defense Center," Lawfare, March 24, 2021, https://www.lawfareblog.com/making-national-cyber-director-operational-national-cyber-defense-center.

27 Peter Singer and August Cole, "A Warning From Tomorrow," n.d., 182.

foreign propaganda and disinformation being waged against the United States and our allies by state and non-state adversaries. Both Senators later introduced an amendment to the Senate's FY 2021 National Defense Authorization Act strengthening these efforts to counter foreign propaganda and disinformation by eliminating the eight-year sunset provision in the authorizing legislation FY 2017 National Defense Authorization Act.

A Director for Information Operations-Offense must be identified without delay, as well, also subordinate to the National Information Operations Director. This position is to coalesce both the means and ends (cyber and its cognitive destination) across the nation in support of Gray Zone and war fighting activities in the information operations environment.

The US Cyber Command should lead this office. US Cyber Command can harness the full breadth of capabilities through pre-existing relationships to support both Department of Defense as well as national objectives. US Cyber Command can achieve this through tasking and partnerships leveraging the Campaign Planning construct that already exists.

In November 2017, the President approved the Unified Command Plan that made US Cyber Command responsible for the planning and executing global cyberspace operations. US Cyber Command's role includes warning and defending against significant cyber-attacks in the United States and its interests and coordinating across the Department of Defense and the United States Government before mounting operations – amongst other responsibilities.

In the version of the FY2018 National Defense Authorization Act, Section 1042 requires the Secretary of Defense to establish processes and procedures to integrate strategic information operations and cyber-enabled information operations across the responsible organizations. It also requires that a senior Department of Defense official implement and oversee such arrangements.

Further, National Security Presidential Memorandum-13, streamlines the process for proposing, evaluating, and approving cyber operations

below the threshold of armed conflict. These reforms have enabled US Cyber Command to implement its strategy of persistent engagement and 'defending forward' in cyberspace.[28] These steps have been vital to creating a more aggressive approach, helping posture US Cyber Command to begin work within the Gray Zone.

In 2018, General Paul Nakasone, Commander, US Cyber Command, identified a new strategic paradigm in cyber operations via increasing resiliency, defending forward, and continuously engaging our adversaries. Of significance, "*Defending Forward* extends reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. Consider the temporal element as a contributing factor to Defend Forward."[29]

US Cyber Command continues to extend its robust cyber strategy via increasing resiliency, defending forward, and continuously engaging its adversaries. A team of global operators are prepared to meet this strategy through cyber effects. While cyber will remain a key capability, this will permit the remaining information operations capabilities to be similarly planned, coordinated, and executed as part of a holistic, coherent, and threat-informed approach. The service components must reorganize to align under US Cyber Command's information operations responsibilities and consistently provide integrated information operations to the joint force and tactical formations.

In January 2021, in preparation for his Senate Armed Services Committee nomination as Secretary of Defense, General Lloyd Austin proclaimed, "The Department of Defense and the US Cyber Command's Cyber Mission Force play a supporting role in greater whole-of-nation efforts to combat foreign influence operations. Department of Defense tools can include cyber effects operations, military information support operations, public outreach, and others. Using combinations of these capabilities in concert with the interagency." Another agency that possesses the same resources, expertise, and broad capabilities, simply does not exist. It would appear to be far easier to embed protocol and standards to

28 "Austin APQs to SASC.Pdf," n.d.

29 "USCYBERCOM Vision April 2018.Pdf," accessed October 20, 2020, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

ensure Department of Defense efforts don't exceed authorities and grant executive authority status than to create a new architecture, with another office, to provide Information Operations-Offense responsibilities.

2. A Fusion Center Must Be Assigned at Both IO Defense and Offense

Congress should identify and fund a Joint Collaborative Environment, or Fusion Center, for both Information Operations-Defense and Offense. This is vital to assure a common and interoperable environment for sharing and fusing data across the relevant information operations functional communities.[30] This common operating environment must provide a real-time view of information and cyber activities across the globe. Both artificial intelligence and big data analysis need to be central enablers at each location. Currently, the community is emphasizing both big data analytics and artificial intelligence with a variety of investments and new initiatives. The data collected include adversarial behavioral modeling, detection of disinformation, inference learning, pattern recognition, etc. Information sharing agreements must be negotiated, defaulting to sharing.

Operations analysis is ab generation of applications that analyze machine data and gain insight from it, improving operational results.[31] As an alternative, artificial intelligence algorithms can potentially use and process data at a previously unrealizable scale, yielding new

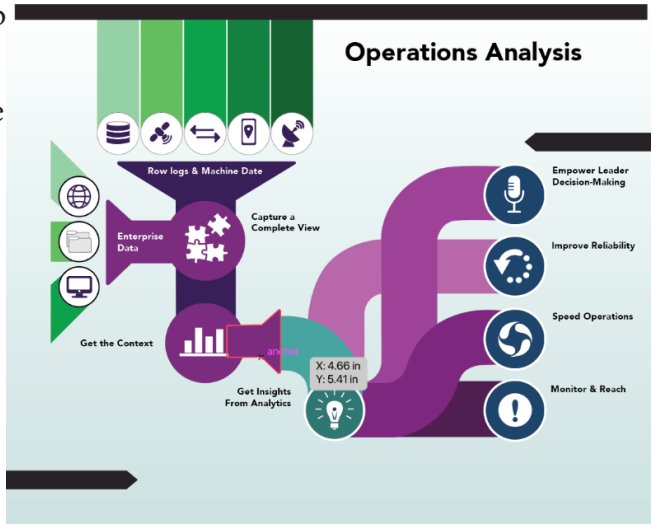

Figure Six: Operations Analysis *Source: IBM*

30 Singer and Cole, "A Warning From Tomorrow."

31 "Operations Big Data Use Cases.Png (1656×1332)," accessed January 11, 2021, https://www.ibmbigdatahub.com/sites/default/files/infographic_file/Operations-Big-Data-Use-Case-3-13-14.png.

findings and potentially new information operations effects.[32] The focus is essentially on taking advantage of massive amounts of computing and storage of computing power and center governance of artificial intelligence and big data analytics around each Fusion Center.

Troubling though, a new report from George Washington University's Center for Cyber and Homeland Security estimates that 99%-plus of the data that Department of Defense collects is likely dark and never exploited.[33] They remain in stovepipes, idle.

The National Information Operations Director should assign both Information Operations - Defense and Offense to identify all Centers-of-Gravity within their mission space and develop information-sharing agreements with security protections that afford privacy, intelligence oversight, and other legal considerations.

An example of a Center-of-Gravity is the National Cyber Investigative Joint Task Force (NCIJTF) who has the primary responsibility to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation."[34] The NCIJTF has sensitive data that could include US Persons or investigative data. However, with legal reviews, masking of data once viewed by a human, secure partitioning of data, and other governance, possibly this is data that could be carefully shared, yielding tremendous discoveries - particularly when applied to artificial intelligence.

There are also private sector initiatives that serve as benchmarks for the expansion of these Fusion Centers. One such example is GDELT (Global Database of Events, Language, and Tone) supported by Google Jigsaw. The GDELT Project monitors the world's broadcast, print, and web news

32 "DoD's Big Bets on Big Data," C4ISRNET, August 8, 2017, https://www.c4isrnet.com/opinion/the-compass/2015/08/25/dod-s-big-bets-on-big-data/.

33 Michael Brett et al., "Artificial Intelligence for Cybersecurity:: Technological and Ethical Implications" (Center for Cyber and Homeland Security at Auburn University, 2017), http://www.jstor.org/stable/resrep21461.

34 "National Cyber Investigative Joint Task Force," Page, Federal Bureau of Investigation, accessed January 13, 2021, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

from nearly every corner of every country in over 100 languages and identifies the people, locations, organizations, themes, sources, emotions, counts, quotes, images, and events driving our global society every second of every day, creating a free open platform for computing on the entire world.[35] Leveraging this type of data assuredly provides new insights on public views and can identify the means and velocity of messaging across the globe.

Figure Seven: The GDELT Project
Source: www.gdeltproject.org/#computing

Also, pleading for attention is the matter of confronting adversarial influence operations. Social media micro-targeting is already one of the more difficult information operations tactics to counter since messages are only seen by select individuals or groups and for a short time. As machines begin to know us better than we know ourselves, adversaries will increasingly identify and target those who are most susceptible to influence. They will then deliver highly personalized content that achieves maximum effectiveness by exploiting individuals' unique characteristics, beliefs, needs, and vulnerabilities.[36] Artificial intelligence integrated within the Fusion Centers will assist in detection and combatting.

The development of artificial intelligence systems is a two-edged sword for democratic societies. On the one hand, artificial intelligence systems will improve human processes and tasks in the online environment, such as detecting disinformation, bots, altered text, images, and manipulated audio and video material. On the other hand, when adversaries adopt the same technologies, they will magnify the effectiveness and scale of information operations.[37] As ideological and geopolitical tensions between democratic and authoritarian states continue to grow, artificial intelligence

35 "The GDELT Project," accessed February 24, 2021, https://www.gdeltproject.org/.

36 Matt Chessen et al., *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy...and What Can Be Done About It*, 2017, http://www.atlanticcouncil.org/images/publications/The_MADCOM_Future_RW_0926.pdf.

37 "How to Win the Battle Over Data," Belfer Center for Science and International Affairs, accessed March 6, 2021, https://www.belfercenter.org/publication/how-win-battle-over-data.

and computational propaganda are likely to become political warfare tools used against democratic societies.[38]

According to research published in *Small Wars and Insurgencies* on the impact, artificial intelligence has on Gray Zone warfare, "fake news reports with realistic fabricated video and audio can be generated with the help of artificial intelligence. Artificial intelligence can be leveraged in various ways to achieve instantaneous and short-term effects, like creating shock and awe, causing panic, and disorder."

Artificial intelligence remains a core technology, that provides game changing capabilities. The Government also continues its investments in artificial intelligence; both at Intelligence Advanced Research Projects Activity (IARPA), as well as at Defense Advanced Research Projects Activity (DARPA). According to IARPA's online website, "Cyber-attack Automated Unconventional Sensor Environment" (CAUSE) aims to develop and test new automated methods that forecast and detect cyber-attacks significantly earlier than existing methods, mostly leveraging artificial intelligence. Congress should increase priority funding to both IARPA and DARPA in support of artificial intelligence applications supporting the full range of information operations activities.

The Department of Homeland Security/Cybersecurity and Infrastructure Security Agency has a well-established and successful process for the development of Fusion Centers and information sharing with both states and metropolitan areas. Cybersecurity and Infrastructure Security Agency has a strong partnership program with the private sector and has built excellent information sharing capability with its customers. The Department of Homeland Security's National Protection and Programs Directorate operates the Cyber Information Sharing and Collaboration Program, which can be an invaluable source of threat information data for private entities, potentially providing them access to government threat information data, including sensitive, classified information.[39]

---

38 Katarina Kertysova, "Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation Is Produced, Disseminated, and Can Be Countered," *Security and Human Rights* 29, no. 1–4 (December 12, 2018): 55–81, https://doi.org/10.1163/18750230-02901005.

39 "HASC - 2018 - Cyber Operations," accessed January 14, 2021, https://congressional-proquest-com.ezp-prod1.hul.harvard.edu/congressional/result/congressional/congdocumentview?accountid=11311&groupid=103838&parmId=17667394D2F&rsId=1766737DEE6.

Department of Homeland Security's Fusion Centers has not been without criticism. The most frequently cited concerns have been incompatibilities in technological infrastructures, incomplete information sharing, inefficiencies and ineffectiveness, and inability to secure privacy when scouring through data.[40]

Rep. Jim Langevin (D-RI) has introduced language in a recent House Bill designed to create a Joint Collaborative Environment at Cybersecurity and Infrastructure Security Agency to allow for cooperative cyber threat analysis as well as build an Integrated Cyber Center at Cybersecurity and Infrastructure Security Agency to lead defensive government cybersecurity operations.[41]

In February 2017, several experts highlighted the necessity of an Information Operations-Offense Fusion Center capability, providing several vectors whereby artificial intelligence is used for offensive purposes. Artificial intelligence can be used to build realistic fabricated video and audio; automated, hyper-personalized disinformation campaigns; automating influence campaigns; denial-of-information bot-driven attacks; and manipulation of information availability.[42]

3. A Whole-of-Nation Framework Must Be Formalized

A whole-of-nation approach must be formalized with an associated framework, authorities, and resources. The primary actors within an Information Operations-Defense framework would include counterintelligence special agents, the private sector, the public, social media, along with other federal agencies and international partners (see Figure Eight).

---

40 Torin Monahan and Neal A. Palmer, "The Emerging Politics of DHS Fusion Centers," *Security Dialogue* 40, no. 6 (December 1, 2009): 617–36, https://doi.org/10.1177/0967010609350314.

41 Charlie Mitchell, "House Defense Policy Bill Clears Committee, Steeped in Cyber Provisions," *Inside the Pentagon's Inside the Air Force* 31, no. 28 (July 10, 2020), http://search.proquest.com/docview/2421914281/citation/DEB914F206FD499EPQ/1.

42 "Malicious Use of AI.Pdf," accessed January 11, 2021, https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217.

Congress should assign the Department of Homeland Security to collaborate with the Department of Justice's Federal Bureau of Investigation to craft an Information Operations-Counterintelligence Plan. Congress should take steps to increase the number of Federal Bureau of Investigation Cyber Assistant Legal Attaches.[43]

Figure Eight: IO Defense Whole-of-Nation Example

Information Operations-Defense is heavily reliant on a robust, *operationalized* counterintelligence presence to assure decisions are made to combat the threat in today's networked environment. The Fourth Amendment, one of the United States Constitution's most significant privacy protections, can often be a critical factor in determining whether the Federal Bureau of Investigation can obtain the evidence needed to pursue national intelligence responses.[44] These issues are often complicated and time-consuming. In the world of information operations, counterintelligence must have the ability to move at warfighting operations speed – operationalizing counterintelligence.[45]

The Federal Bureau of Investigation is often key in identifying whether an information operations activity resolves to a US Person or foreign entity. This is to prevent inadvertent spying of United States citizens by our intelligence community. However, the processes of assigning attribution can be dilatory. Therefore, rapid *operationalization* of Federal Bureau of Investigation decision-making, the ability to convert from their law enforcement authorities to counterintelligence/national security authorities, become a key factor in information operations success.

43 Singer and Cole, "A Warning From Tomorrow."

44 Greiman, "Public/Private Partnerships in Cyberspace."

45 *Operationalizing CI* clearly reflects a vision that doesn't compromise legal procedures. *Operationalizing* simply refers to making rapid decisions, within the rule of law, yet exploiting attack vectors when possible to achieve IO effects. *Operationalizing CI* is already occurring, but with a legal framework to which to operate, should further accelerate decision-making under the recognition that we are operating in the gray zone, near warfare.

The May 2009 Cyberspace Policy specifically tasked the counterintelligence community to develop and implement a government-wide Cyber Counterintelligence Plan. This plan was to coordinate activities across all federal agencies to detect, deter, and mitigate foreign-sponsored cyber-intelligence threats to the United States and private sector information systems.[46] Remarkably, these critical initiatives have never been enacted into law and do not require congressional oversight. Part of the Comprehensive National Cybersecurity Initiative provides the genesis to require Federal Bureau of Investigation activities to collectively build an information operations counterintelligence plan that could address operationalizing decision-making.

Federal Bureau of Investigation Director Christopher Wray delivered remarks for the 2020 Cybersecurity and Infrastructure Security Agency National Cybersecurity Summit on September 16, 2020. Here, he highlighted the Federal Bureau of Investigation's recently developed strategy involving a focus on partnerships, capabilities, and leveraging authorities. He recognized that the Federal Bureau of Investigation in the past had been centered on combating cyber threats through pure legal measures, one at a time, like "whack-a-mole." The Federal Bureau of Investigation's new strategy, he professes, is more multi-directional, involving the goal of imposing more risk and consequences on our adversaries.

The private sector possesses some of the countries' most advanced, innovative capabilities to detect and confront information operations' threats. However, the private sector does not have the authority to reach beyond the defense of their own network. Despite autocracies having such clear advantages in cyber and information operations, the United States has its own excellent strengths. Our leverage is the strength of our democracy, capitalism, and innovation. We must bring our top talent from Silicon Valley and many other locations across the United States to outflank the threats. This is where our true strength lies. We must have a real collaboration that includes innovative commercial business partners

46 Greiman, "Public/Private Partnerships in Cyberspace."

- from national policy to support to new technologies, analysis, and defensive execution.[47]

On August 6, 2013, the White House released a list of eight potential incentives the government might offer to encourage companies to adopt the National Institute of Standards and Technology's cybersecurity framework and enhance information sharing, including liability protection, insurance, and cybersecurity conditions in government grants.[48] Additionally, in 2016, former homeland security and intelligence officials from both the Bush and Obama administrations had backed a report entitled, "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats" which laid out a policy framework for companies to actively defend against foreign hackers, including a recommendation for government "certification" of private organizations. This bipartisan task force published 15 policy recommendations centering its findings on a call for the Department of Justice to issue guidance on the current legal limits for an active cyber defense by the private sector.[49]

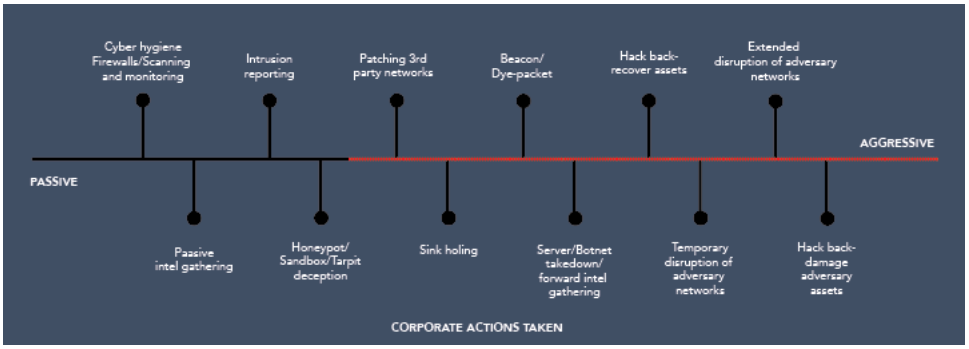

Figure Nine: Corporate Cyber Defense *Source: The Private Sector and Active Defense Cyber Threats*

The United States industry is eager to be provided new authorities, or even incentives, to properly defend not only their information and network, but many are patriots wanting to contribute to larger national interests, without breaching authorities. Figure Nine highlights along the horizontal line in black, those roles the private sector has already achieved with success. The horizontal line in red are those activities the private sector possesses the

47 Mark Testoni (CEO, SAP National Security Services) in discussion with the author, January 28, 2021.

48 "Incentives to Support Adoption of the Cybersecurity Framework," whitehouse.gov, August 6, 2013, https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

49 "2016 - Certify Companies For Active Defense.Pdf," accessed February 5, 2021, https://illiad.hul.harvard.edu/illbasicauth/HUL/pdf/5918701.pdf.

skill to pursue, but awaits permissions. Government must begin weighing the private sector's role, and assuredly, if that role is extended in a careful and deliberate fashion, policies and oversight must be in place.

Further cementing the private sector role, the 2021 National Defense Authorization Act (Sec. 1631) requires the Secretary of Defense to establish a threat intelligence sharing program and obtain threat intelligence from the defense industrial base.[50] Such a program must be mandated. The report further stated that there must be innovative methods to extend to all the private sectors' ability to defend themselves and contribute to governmental actions.

Finally, in March 2021, in a reaction to the SolarWinds hack, during a rare Senate Armed Services Committee Hearing, private companies, lawmakers, intelligence officials, and the White House have all called for greater information sharing between the private and public sectors – potentially through a clearinghouse model where private and public sector intelligence is funneled into one central repository, likely overseen by the Department of Homeland Security.[51]

Information Operations-Defense must identify cybersecurity mandates needing legislation, as well as potential incentives, to build a formal 'Information Operations-Defense Citizen Team' supporting information sharing, threat intelligence, and other initiatives. In a 2020 Cybersecurity Summit, former Director of Homeland Security Michael Chertoff noted, "What has changed most recently is social media, and the ability to drive very carefully tailored messages to particular individuals.[52]

Information Operations-Defense should also expand its work with the private sector on measures to help the American people become savvier consumers of information.[53] And job number one is to get people to be

50 "2021 NDAA.Pdf," n.d.

51 Tonya Riley, "Analysis | The Cybersecurity 202: NSA Director Says Intelligence Has a Big Blind Spot: Domestic Internet Activity," *Washington Post*, accessed March 30, 2021, https://www.washingtonpost.com/politics/2021/03/26/cybersecurity-202-nsa-director-says-intelligence-has-big-blind-spot-domestic-internet-activity/.

52 Washington Post Live, "Transcript: Cybersecurity Summit," *Washington Post*, accessed February 5, 2021, https://www.washingtonpost.com/washington-post-live/2019/10/04/transcript-cybersecurity-summit/.

53 Chessen et al., *The MADCOM Future*.

critical in their thinking when they see a story and not simply accept that it's true because "it's on the Internet." Here, the citizenry needs to become involved.

What's Next?

It's often said that significant change requires three things: 1) to understand the problem; 2) to provide a solution that makes sense and creates synergies; and 3) most importantly, to have the political will – someone who can carry the torch. The torch has been lit by US companies who have lost their market share and intellectual edge; citizens who have lost their privacy and right to truth; and the government which finds itself much closer to war and further from national financial security due to adversarial information operations. My hope is that policymakers will take an interest in this research and consider the merits of the approach I propose.

It is impossible to anticipate precisely what is needed to combat the threats we see in the information environment. One thing is clear for sure. The threat is getting more ubiquitous and aggressive, migrating from unidirectional cyber-attacks towards a multi-dimensional targeting across the physical, to virtual, to cognitive space of the information environment. U.S. capabilities in network activities are powerful, and maybe unparalleled. However, in the broader sense, the U.S. is trailing in evolution to address the full range of the information threat that extends to the human mind. If we don't act soon, what comes after the reckoning won't be palatable.

What Would The Reckoning Have Looked Like If This Strategy Had Been In Place?

Had this next-generation national information operations strategy & architecture been implemented from the onset, I believe the results from the initial scenario, entitled "*The Reckoning,*" would have had a substantially different outcome. The public would have been better attuned to what disinformation looks like and equipped to critically analyze and report disinformation. Both Information Operations-Defense and Offense will possess the latest artificial intelligence advancements in support of identifying and repelling malicious bots, posts, and other network traffic. The private sector would lean forward, with proper oversight, providing advanced analysis of the latest threats. Also, possessing some of the nation's most expert cyber professionals, the private sector coordinates under a new agreement, the conduct of *sink-holing* and *beaconing* passive activities in support of government direction to support attribution and defense. The counterintelligence community, embedded within each Fusion Center, has operationalized their decision-making, based on new legal interpretations and is able to support war fighting and Gray Zone interests at near real time. Information Operations-Offense at US Cyber Command, fed with intelligence powered by artificial intelligence, immediately recognizes the visit by Chinese President Xi as simply white noise, to disguise an already recognized objective. The National Information Operations Director is informed and directs a campaign plan. The President is briefed and gives orders to the US Pacific Fleet to deploy the full weight of the 7th Fleet in the protection of Taiwan. The crisis is averted. President Xi returns to China with his head down in confusion.

Glossary

Active Measures Activities undertaken to achieve foreign policy objectives by state-sponsored influence operations targeting citizenry, influence operations between nations, and population-to-population influence operations.

Artificial Intelligence Artificial intelligence is the ability of a system to perform tasks characteris-tic of human intelligence, such as learning and decision-making. Machine learning (ML), not to be confused with AI, can be generally defined as the usage of algorithms and large datasets to train computer systems to recognize patterns that had not previously been defined, and the ability of these systems to learn from data and discern valuable information without being programmed ex-plicitly to do so.

Computational Propaganda A new term for the use of social media, big data, autonomous agents, and related technologies for political manipulation. This can range from relatively benign amplification of political messages to insidious state-sponsored trolling and disinformation. The web robot, or "bot," is the most common type of autonomous agent used in computational propa-ganda. Bot capabilities are limited to providing basic answers to simple questions, publishing con-tent on a schedule, or disseminating content in response to triggers. However, bots can have a dis-proportionate impact because it is easy to create a lot of them, bots post content with high volume and high frequency, and their profiles are typically designed to imitate their target population of human beings.

Cyberspace Department of Defense defines cyberspace as an "interdependent network of infor-mation technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Disinformation Unlike misinformation, disinformation is intentionally false. Examples include planting deliberately false news stories in the

media, manufacturing protests, doctoring pictures, and tampering with private and/or classified communications before their widespread release.

Gray Zone Warfare Techniques to achieve a nation's goals while denying those of its rivals by employing instruments of power that do not necessarily include the use of acknowledged regular military forces. These may involve state and non-state actors and fall between traditional wars and peacetime. Gray zone warfare entails techniques to achieve a nation's goals while denying those of its rivals by employing instruments of power that do not necessarily include the use of acknowl-edged regular military forces. These may involve state and non-state actors and fall between traditional wars and peacetime.

Hybrid warfare Blends conventional, irregular, and information warfare. It may also include eco-nomic and other forms of competition and contention. Often used to describe information warfare, hybrid warfare encompasses activities that fall outside of the information warfare rubric.

Information Environment The aggregation of individuals, organizations, and systems that col-lect, disseminate, or act on information. This includes:

- Physical Layer: Command and control systems and associated infrastructure.
- Informational Layer: Networks and systems where information is stored.
- Cognitive Layer: The minds of people who transmit and respond to information.

Information-Related Capabilities Constitute tools, techniques, or activities employed within a dimension of the information environment that can be used to achieve a specific end at a specific time and place. IRCs can include, but are not be limited to, a variety of technical and non-technical activities that intersect the traditional areas of electronic warfare, cyberspace operations, military information support operations, military deception, influence activities, operations security, and in-telligence.

Military Deception Actions to deliberately mislead adversary military, paramilitary, or violent ex-tremist organization decision-makers, thereby causing the adversary to take specific actions (or in-actions) that will contribute to the accomplishment of the friendly mission. A pillar closely related to psychological operations, military deception focuses on false information or disinformation.

Misinformation This is the spreading of unintentionally false information. Examples include in-ternet trolls who spread unfounded conspiracy theories or web hoaxes through social media, be-lieving them to be true. Misinformation can have the effect of sowing divisiveness and chaos in a target society, as the truth becomes harder to discern.

Propaganda This is the propagation of an idea or narrative that is intended to influence, like psy-chological or influence operations. It can be misleading but true and may include stolen infor-mation. A government communicating its intent, policies, and values through speeches, press re-leases, and other public affairs can be considered propaganda as well as public diplomacy. These communications have strategic value in that over time they can create perceptions that steer deci-sion-makers towards a certain course of action.

Psychological Operations Now is known as Military Information Support Operations. These are operations planned to convey selected information and indicators to influence the emotions, mo-tives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

Soft Power The ability to get what you want through attraction rather than coercion or payments." This may involve the use of information with a positive spin to compel decision-makers toward actions in one's interests.

Bibliography

"2013 National Infrastructure Protection Plan.Pdf." Accessed January 6, 2021. https://permanent.fdlp.gov/gpo147129/national-infrastructure-protection-plan-2013-508.pdf.

"2016 - Certify Companies For Active Defense.Pdf." Accessed February 5, 2021. https://illiad.hul.harvard.edu/illbasicauth/HUL/pdf/5918701.pdf.

"2016 - Clapper-Lettre-Rogers.Pdf." Accessed January 6, 2021. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

"2018 - ATP 3-13-1 (Conduct of Information Operations).Pdf." Accessed January 11, 2021. https://fas.org/irp/doddir/army/atp3-13-1.pdf.

"2018 - Cyber Strategy Summary." Accessed October 20, 2020. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

"2018 - HASC Hearing - Influence Operations.Pdf." Accessed February 5, 2021. https://illiad.hul.harvard.edu/illbasicauth/HUL/pdf/5913416.pdf.

"2021 - IWP - The Application of International Law to Cyber Operations. Ppt," n.d.

"2021 - SASC Preparation - Austin.Pdf," n.d.

"2021 NDAA.Pdf," n.d.

"ARMY Digitalization." States News Service. 2020.

Brett, Michael, George Duchak, Anup Ghosh, Kristin Sharp, Frank J. Cilluffo, and Sharon L. Cardash. "Artificial Intelligence for Cybersecurity:: Technological and Ethical Implications." Center for Cyber and Homeland

Security at Auburn University, 2017. http://www.jstor.org/stable/resrep21461.

Belfer Center for Science and International Affairs. "Can Democracy Survive in the Information Age?" Accessed January 7, 2021. https://www.belfercenter.org/publication/can-democracy-survive-information-age.

"CAUSE." Accessed February 24, 2021. https://www.iarpa.gov/index.php/research-programs/cause.

Chen, J. "On Levels of Deterrence in the Cyber Domain." Journal of Information Warfare 17, no. 2 (2018): 32–41. https://doi.org/10.2307/26633152.

Chessen, Matt, Atlantic Council of the United States, Brent Scowcroft Center on International Security, Atlantic Council of the United States, and Dinu Patriciu Eurasia Center. The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy...and What Can Be Done About It, 2017. http://www.atlanticcouncil.org/images/publications/The_MADCOM_Future_RW_0926.pdf.

"CI Threat Information Framework.Pdf." Accessed January 13, 2021. https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf.

"CISA Homepage." Accessed January 13, 2021. https://www.cisa.gov/.

"Conflict Management and 'Whole of Government.'" Accessed August 30, 2020. https://permanent.fdlp.gov/websites/ssi.armywarcollege.edu/pubs/display.cfm-pubID=1102.htm.

CyberScoop. "Congress Moves on NDAA - Loaded with Cyber Provisions," December 7, 2020. https://www.cyberscoop.com/congress-solarium-commission-defense-authorization-ndaa/.

Conley, Bill, John Stine, Adam Miller, and Brig Gen Lance Landrum. "DOD's Broad Vision for Electromagnetic Battle Management." Journal of Electronic Defense 42, no. 9 (September 2019): 36–41.

Corker, Bob, James E Risch, Marco Rubio, Ron Johnson, Jeff Flake, Cory Gardner, Todd Young, et al. "Committee on Foreign Relations - Putin's Asymmetric Threat," n.d., 206.

"DC3 - Fact Sheet.Pdf." Accessed January 13, 2021. https://www.dc3.mil/Portals/100/Documents/DC3/Resources/Factsheets/DC3-FactSheet-20NOV2020.pdf.

"Democracy in China." In Wikipedia, December 13, 2020. https://en.wikipedia.org/w/index.php?title=Democracy_in_China&oldid=993952049.

"DHS-Cybersecurity-Strategy.Pdf." Accessed December 9, 2020. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

"Digital Attack Map." Accessed January 23, 2021. https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17982&view=map.

Federal Bureau of Investigation. "Director Wray Addresses CISA Cybersecurity Summit - 2020." Video. Accessed February 5, 2021. https://www.fbi.gov/video-repository/wray-cisa-091620.mp4/view.

SIGNAL Magazine. "Disruptive by Design: Transcending Cyber," January 25, 2021. https://www.afcea.org/content/disruptive-design-transcending-cyber.

Dobson, GB, A Rege, and KM Carley. "Informing Active Cyber Defence with Realistic Adversarial Behavior." Journal of Information Warfare 17, no. 2 (2018): 16–31. https://doi.org/10.2307/26633151.

"DoD Counterintelligence. DODD-5240.2." Accessed December 8, 2020. https://fas.org/irp/doddir/dod/dodcount.htm.

"DoD Strategy for Operations in the IE.Pdf." Accessed January 8, 2021. https://permanent.fdlp.gov/gpo82473/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

"DODD 360001.Pdf." Accessed January 8, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf?ver=2019-08-12-094732-187.

"DODD 524001.Pdf." Accessed December 8, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524001p.pdf.

C4ISRNET. "DoD's Big Bets on Big Data," August 8, 2017. https://www.c4isrnet.com/opinion/the-compass/2015/08/25/dod-s-big-bets-on-big-data/.

Duvenage, PC, VJ Jaquire, and SH von Solms. "Towards a Literature Review on Cyber Counterintelligence." Journal of Information Warfare 17, no. 4 (2018): 11–25. https://doi.org/10.2307/26783824.

"Enemy Cyber Campaigns Target Private Sector - ProQuest." Accessed August 30, 2020. http://search.proquest.com/docview/1958843300?accountid=11311&rfr_id=info%3Axri%2Fsid%3Aprimo.

Farwell, James P. Information Warfare - Forging Communication Strategies for 21st Century Operational Environments. Quantico, VA: Marine Corps University Press, 2020.

Auburn University. "FBI Unveils Revised Cyber Security Strategies - Auburn." Accessed February 5, 2021. http://ocm.auburn.edu/newsroom/news_articles/2020/10/011540-fbi-cyber-security-panel.php.

FDD. "FDD | U.S. Government and Private Industry Must Prepare for Cyber-Enabled Economic Warfare Escalations," February 5, 2019. https://

www.fdd.org/analysis/2019/02/05/government-and-private-industry-must-prepare-for-cyber-enabled-economic-warfare-escalations/.

Fritsch, L, and S Fischer-Hübner. "Implications of Privacy & Security Research for the Upcoming Battlefield of Things." Journal of Information Warfare 17, no. 4 (2018): 72–87. https://doi.org/10.2307/26783828.

Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen. "State, Media, and Civil Society in the Information Warfare over Ukraine." International Affairs 94, no. 5 (September 1, 2018): 975–94. https://doi.org/10.1093/ia/iiy148.

GovData360. "GovData360 - Trustworthiness and Confidence." Accessed January 17, 2021. https://govdata360.worldbank.org/indicators/h86ecbc30?country=BRA&indicator=41321&viz=line_chart&years=2007,2017.

Greiman, VA. "Public/Private Partnerships in Cyberspace: Building a Sustainable Collaboration." Journal of Information Warfare 14, no. 3 (2015): 30–42.

"HASC - 2018 - Cyber Operations." Accessed January 14, 2021. https://congressional-proquest-com.ezp-prod1.hul.harvard.edu/congressional/result/congressional/w?accountid=11311&groupid=103838&parmId=17667394D2F&rsId=1766737DEE6.

"HASC on Intelligence Hearing - FY21 - Budget Request - USCYBERCOM and Cyberspace Operations." Accessed December 10, 2020. https://congressional-proquest-com.ezp-prod1.hul.harvard.edu/congressional/result/congressional/w?accountid=11311&groupid=103838&parmId=175B2FD706F&rsId=175B2FD5727.

Hatch, Ben. "The Future of Strategic Information and Cyber-Enabled Information Operations." Journal of Strategic Security 12, no. 4 (January 2019): 69–89. https://doi.org/10.5038/1944-0472.12.4.1735.

Helms, Christian P. "The Digital GCC: USCYBERCOM As a Combatant Command:" Fort Belvoir, VA: Defense Technical Information Center, April 1, 2015. https://doi.org/10.21236/AD1012758.

Henriques, J, F Caldeira, T Cruz, and P Simões. "On the Use of Ontology Data for Protecting Critical Infrastructures." Journal of Information Warfare 17, no. 4 (2018): 38–55. https://doi.org/10.2307/26783826.

Hoehn, John R. "U.S. Military Electronic Warfare Program Funding: Background and Issues for Congress," n.d., 17.

Defense One. "How to Stop Losing the Information War." Accessed January 8, 2021. https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/.

Belfer Center for Science and International Affairs. "How to Win the Battle Over Data." Accessed March 6, 2021. https://www.belfercenter.org/publication/how-win-battle-over-data.

Hurley, JS. "Enabling Successful Artificial Intelligence Implementation in the Department of Defense." Journal of Information Warfare 17, no. 2 (2018): 65–82. https://doi.org/10.2307/26633155.

"IARPA Research - CAUSE." Accessed February 24, 2021. https://www.iarpa.gov/index.php/research-programs/cause.

whitehouse.gov. "Incentives to Support Adoption of the Cybersecurity Framework," August 6, 2013. https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

Information Warfare. 1st ed. John Wiley & Sons, Ltd, 2016. https://doi.org/10.1002/9781119004721.

The Lightning Press SMARTbooks. "Instruments of National Power," September 20, 2014. https://www.thelightningpress.com/the-instruments-of-national-power/.

"Joint Concept Integrated Campaign.Pdf." Accessed January 4, 2021. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.

"Joint Concepts - Operating in the Information Environment.Pdf." Accessed December 31, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.

"Joint Publication 3-12.Pdf." Accessed December 7, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

"Joint Publication 3-13.Pdf." Accessed December 7, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

Jr, Sydney J. Freedberg. "Army Unveils Hacker HQ For Offensive Cyber, Info War." Breaking Defense (blog). Accessed February 23, 2021. https://breakingdefense.com/2020/09/army-unveils-hacker-hq-for-offensive-cyber-info-war/.

Karas, Rachel S. "DoD Driving Toward New Electromagnetic Spectrum Battle Management Ideas." Inside the Pentagon's Inside Missile Defense 23, no. 26 (December 20, 2017). http://search.proquest.com/docview/1978601649/abstract/C6C3C89DE2E54D1EPQ/1.

Kertysova, Katarina. "Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation Is Produced, Disseminated, and Can Be Countered." Security and Human Rights 29, no. 1–4 (December 12, 2018): 55–81. https://doi.org/10.1163/18750230-02901005.

Kimminau, Jon A. "Five Examples of Big Data Analytics and the Future of ISR," n.d., 2.

Larson, Eric V., and United States, eds. Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities. Rand Corporation Monograph Series. Santa Monica, CA: Rand Arroyo Center, 2009.

Lee, Sheila Jackson, James R Langevin, Cedric L Richmond, Kathleen M Rice, J Luis Correa, Xochitl Torres Small, Lauren Underwood, et al. "Committee on Homeland Security - FY20 Budget Request," n.d., 50.

"Leithauser, T. (2011). Federal Agencies Need to Share More Cyber Threat Data, Audit Says. Cybersecurity Policy Report, N," n.d.

Libicki, Martin C. "The Convergence of Information Warfare." Strategic Studies Quarterly: SSQ 11, no. 1 (Spring 2017): 49–65.

Lin, Herbert, and Amy B. Zegart, eds. Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations. Washington, D.C: Brookings Institution Press, 2018.

Live, Washington Post. "Transcript: Cybersecurity Summit." Washington Post. Accessed February 5, 2021. https://www.washingtonpost.com/washington-post-live/2019/10/04/transcript-cybersecurity-summit/.

"Malicious Use of AI.Pdf." Accessed January 11, 2021. https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217.

"Maneuvering in the Information Environment.Com." Accessed December 31, 2020. https://jellevanhaaster.com/index.php/portfolio/manoeuvring-and-generating-effects-in-the-information-environment/.

Mccaul, Michael T, Lamar Smith, Peter T King, Mike Rogers, Paul C Broun, Patrick Meehan, South Carolina, et al. "Committee on Homeland Security - DHS Cybersecurity," n.d., 78.

McClintock, Bruce. "Russian Information Warfare: A Reality That Needs a Response," July 21, 2017. https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html.

Media, O'Reilly. "Cyberwar and Information Warfare." Accessed September 20, 2020. http://learning.oreilly.com/library/view/cyberwar-and-information/9781118603512/02_tableofcontents.html.

———. “Cyberwar and Information Warfare - Cyberwar and Information Warfare.” Accessed August 29, 2020. https://learning-oreilly-com.ezp-prod1.hul.harvard.edu/library/view/cyberwar-and-information/9781118603512/02_tableofcontents.html.

———. “Global Information Warfare, 2nd Edition.” Accessed February 24, 2021. http://learning.oreilly.com/library/view/global-information-warfare/9781498703260/.

———. “Introduction to Cyber-Warfare.” Accessed August 30, 2020. http://learning.oreilly.com/library/view/introduction-to-cyber-warfare/9780124078147/.

Mitchell, Charlie. “House Defense Policy Bill Clears Committee, Steeped in Cyber Provisions.” Inside the Pentagon’s Inside the Air Force 31, no. 28 (July 10, 2020). http://search.proquest.com/docview/2421914281/citation/DEB914F206FD499EPQ/1.

Molander, Roger C., Andrew Riddile, and Peter A. Wilson. “Strategic Information Warfare: A New Face of War,” December 31, 1995. https://www.rand.org/pubs/monograph_reports/MR661.html.

Monahan, Torin, and Neal A. Palmer. “The Emerging Politics of DHS Fusion Centers.” Security Dialogue 40, no. 6 (December 1, 2009): 617–36. https://doi.org/10.1177/0967010609350314.

Myers, Elizabeth A. “Cyber as a ‘Team Sport’: Operationalizing a Whole-of-Government Approach to Cyberspace Operations,” n.d., 120.

Federal Bureau of Investigation. “National Cyber Investigative Joint Task Force.” Page. Accessed January 13, 2021. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

“National Cyber Strategy.Pdf.” Accessed October 20, 2020. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"NATO IO.Pdf." Accessed December 31, 2020. https://info.publicintelligence.net/NATO-IO.pdf.

Niekerk, Brett Van, and Manoj S. Maharaj. "Relevance of Information Warfare Models to Critical Infrastructure Protection." Scientia Militaria - South African Journal of Military Studies 39, no. 2 (November 5, 2011). https://doi.org/10.5787/39-2-114.

Norton, Helen L. "The Government's Lies and the Constitution," n.d., 50.

"ODNI on Accountability." Accessed January 10, 2021. https://www.dni.gov/index.php/how-we-work/accountability.

"Operational Decision Making for Cyber Operations.Pdf," n.d.

"Operations Big Data Use Cases.Png (1656×1332)." Accessed January 11, 2021. https://www.ibmbigdatahub.com/sites/default/files/infographic_file/Operations-Big-Data-Use-Case-3-13-14.png.

Pahi, T, M Leitner, and F Skopik. "Preparation, Modelling, and Visualisation of Cyber Common Operating Pictures for National Cyber Security Centres." Journal of Information Warfare 16, no. 4 (2017): 26–40.

Pal, PP, NJ Lageman, and NB Soule. "Disrupting Adversary Decision Logic: An Experience Report." Journal of Information Warfare 17, no. 3 (2018): 78–91. https://doi.org/10.2307/26633167.

Paterson, Thomas, and Lauren Hanley. "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes.'" Australian Journal of International Affairs 74, no. 4 (July 3, 2020): 439–54. https://doi.org/10.1080/10357718.2020.1734772.

"Pence: China Engaged in Cyber-Backed, Whole-of-Government Campaign Against US." Accessed August 30, 2020. http://search.proquest.com/docview/2117351077?accountid=11311&rfr_id=info%3Axri%2Fsid%3Aprimo.

"Pentagon Urges Whole-of-Government Response to China's Cyber." Accessed August 30, 2020. http://search.proquest.com/docview/2167289852?accountid=11311&rfr_id=info%3Axri%2Fsid%3Aprimo.

"Policy for US Cybersecurity." Accessed August 30, 2020. http://search.proquest.com/docview/1652188677?accountid=11311&rfr_id=info%3Axri%2Fsid%3Aprimo.

Reber, PA, and SR Graham. "Evaluating System on a Chip Design Security." Journal of Information Warfare 16, no. 3 (2017): 63–78.

"Regulating the Battlefield of the Future: Legal Limitations on Psychological Operations." Accessed January 5, 2021. https://go-gale-com.ezp-prod1.hul.harvard.edu/ps/i.do?p=LT&u=camb55135&id=GALE|A147746244&v=2.1&it=r.

Robertson, Jordan, and Michael Riley. "The Long Hack: How China Exploited a U.S. Tech Supplier," n.d., 22.

Russell, SL, and SC Jackson. "Operating in the Dark: Cyber Decision-Making from First Principles." Journal of Information Warfare 17, no. 1 (2018): 1–15. https://doi.org/10.2307/26504126.

Sanger, David E., Nicole Perlroth, and Julian E. Barnes. "As Understanding of Russian Hacking Grows, So Does Alarm." The New York Times, January 2, 2021, sec. U.S. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Sang-Hun, Choe. "North Korea Launches Missile, but Test Appears to Fail." The New York Times, March 22, 2017, sec. World. https://www.nytimes.com/2017/03/22/world/asia/north-korea-missile-launch-failure.html.

"SASC Committee Hearing - USCYBERCOM.Pdf." Accessed January 7, 2021. https://illiad.hul.harvard.edu/illbasicauth/HUL/pdf/5913314.pdf.

Schneier, Bruce. "Opinion - Why Was SolarWinds So Vulnerable to a Hack?" The New York Times, February 23, 2021, sec. Opinion. https://www.nytimes.com/2021/02/23/opinion/solarwinds-hack.html.

Shaji, Ramaswamy Swarnammal, V. Sachin Dev, and Thomas Brindha. "A Methodological Review on Attack and Defense Strategies in Cyber Warfare." Wireless Networks 25, no. 6 (August 1, 2019): 3323–34. https://doi.org/10.1007/s11276-018-1724-1.

Silomon, JAM. "Software as a Weapon: Factors Contributing to the Development and Proliferation." Journal of Information Warfare 17, no. 3 (2018): 106–23. https://doi.org/10.2307/26633169.

Singer, Peter, and August Cole. "A Warning From Tomorrow," n.d., 182.

Smeets, Max, and Jd Work. "Operational Decision Making for Cyber Operations: In Search of a Model." Preprint. SocArXiv, September 15, 2019. https://doi.org/10.31235/osf.io/xwrhk.

"Statevote 2012." Accessed January 13, 2021. https://www.ncsl.org/research/elections-and-campaigns/statevote.aspx.

Stefanik, Elise M, Bill Shuster, Brad R Wenstrup, Ralph Lee Abraham, Liz Cheney, Joe Wilson, South Carolina, et al. "HASC - Emerging Threats (2017)," n.d., 88.

———. "Subcommittee on Emerging Threats and Capabilities," n.d., 72.

Steve Abrams. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." Connections. The Quarterly Journal (English Ed.) 15, no. 1 (2016): 5–31. https://doi.org/10.11610/Connections.15.1.01.

"Strategic Counterintelligence - An Approach to Engaging Security Threats," n.d., 111.

Sulmeyer, Michael. "Campaign Planning with Cyber Operations." Georgetown Journal of International Affairs 18, no. 3 (2017): 131–37. https://doi.org/10.1353/gia.2017.0045.

"The 2018 National Defense Strategy: Continuity and Competition - ProQuest." Accessed December 7, 2020. http://search.proquest.com/docview/2166946492?accountid=11311&pq-origsite=primo.

"The GDELT Project." Accessed February 24, 2021. https://www.gdeltproject.org/.

Lawfare. "The NDAA's National Cyber Director: Justifications, Authorities, and Lingering Questions," December 7, 2020. https://www.lawfareblog.com/ndaas-national-cyber-director-justifications-authorities-and-lingering-questions.

The Strategy Bridge. "The United States National Security Council Needs an Information Warfare Directorate." Accessed January 1, 2021. https://thestrategybridge.org/the-bridge/2019/12/3/the-united-states-national-security-council-needs-an-information-warfare-directorate.

War on the Rocks. "The United States Needs an Information Warfare Command: A Historical Examination," June 14, 2019. https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/.

Theohary, Catherine A. "Defense Primer: Information Operations," n.d., 3.

———. "Information Warfare: Issues for Congress." Information Warfare, n.d., 19.

Thomas, Timothy L. Dragon Bytes: Chinese Information War Theory and Practice. Fort Leavenworth, Kan.: Foreign Military Studies Office, 2004.

Tom Leithauser. "Federal Agencies Need to Share More Cyber Threat Data Audit Says." Cybersecurity Policy Report, 2011, N_A-.

Towell, Pat, Lynn M Williams, Andrew Feickert, Jeremiah Gertler, Steven A Hildreth, Kristy N Kamarck, Lawrence Kapp, et al. "FY2018 National Defense Authorization Act," n.d., 45.

"USCYBERCOM Cyberspace Strategy Symposium Proceedings 2018.Pdf." Accessed October 20, 2020. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.

"USCYBERCOM Vision April 2018.Pdf." Accessed October 20, 2020. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

"Using Machine Learning to Detect Malign Information Efforts Online." Accessed January 6, 2021. https://www.rand.org/randeurope/research/projects/using-machine-learning-to-detect-malign-information-efforts.html.

"What Is Big Data.Pdf." Accessed January 11, 2021. https://www.oracle.com/a/ocom/docs/what-is-big-data-ebook-4421383.pdf?elqTrackId=a1ac9abe0b194b448851165468e3fe5e&elqaid=87688&elqat=2.

"With New Cyber Strategy, DoD Aims to 'Defend Forward' - ProQuest." Accessed October 20, 2020. http://search.proquest.com/docview/2123609137?accountid=11311&rfr_id=info%3Axri%2Fsid%3Aprimo.

Yan, Guilong. "The Impact of Artificial Intelligence on Hybrid Warfare." Small Wars & Insurgencies 31, no. 4 (May 18, 2020): 898–917. https://doi.org/10.1080/09592318.2019.1682908.

Ziegler, Charles E. "International Dimensions of Electoral Processes - Russia, the USA, and the 2016 Elections." International Politics 55, no. 5 (September 1, 2018): 557–74. https://doi.org/10.1057/s41311-017-0113-1.

National Security Fellows Program
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/NSF